

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
21 December 2000 (21.12.2000)

PCT

(10) International Publication Number  
**WO 00/77585 A1**

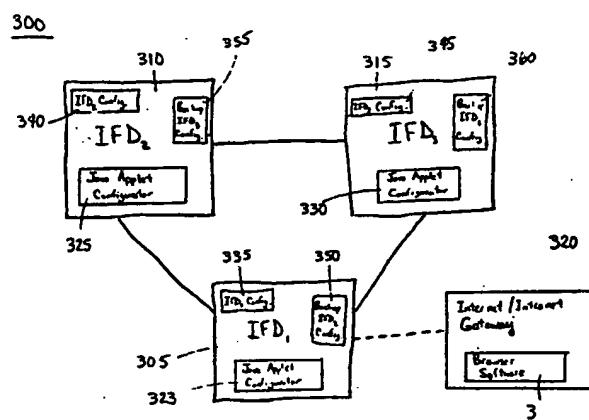
- (51) International Patent Classification<sup>7</sup>: **G05B 19/042, 19/05**
- (21) International Application Number: **PCT/US00/15894**
- (22) International Filing Date: **12 June 2000 (12.06.2000)**
- (25) Filing Language: **English**
- (26) Publication Language: **English**
- (30) Priority Data:
- |            |                             |    |
|------------|-----------------------------|----|
| 60/139,071 | 11 June 1999 (11.06.1999)   | US |
| 60/144,693 | 20 July 1999 (20.07.1999)   | US |
| 60/149,276 | 17 August 1999 (17.08.1999) | US |
| 09/531,597 | 20 March 2000 (20.03.2000)  | US |
- (63) Related by continuation (CON) or continuation-in-part (CIP) to earlier applications:
- |          |                             |
|----------|-----------------------------|
| US       | 60/139,071 (CIP)            |
| Filed on | 11 June 1999 (11.06.1999)   |
| US       | 60/144,693 (CIP)            |
| Filed on | 20 July 1999 (20.07.1999)   |
| US       | 60/149,276 (CIP)            |
| Filed on | 17 August 1999 (17.08.1999) |
| US       | 09/531,597 (CIP)            |
| Filed on | 20 March 2000 (20.03.2000)  |
- (71) Applicant (for all designated States except US): **INVENTSYS PLC [US/US]; 33 Commercial Street, Foxboro, MA 02035 (US).**
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **ADAMS, Lloyd [US/US]; Invensys plc, 33 Commercial Street, Foxboro, MA 02035 (US). JOHNSON, Alexander [US/US]; Invensys plc, 33 Commercial Street, Foxboro, MA 02035 (US).**
- (74) Agents: **HAYDEN, John, F; Fish & Richardson, P.C., 601 Thirteenth Street, N.W., Washington, D C 20005 et al. (US).**
- (81) Designated States (national): **AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.**
- (84) Designated States (regional): **ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European**

[Continued on next page]

(54) Title: PEER-TO-PEER HOSTING OF INTELLIGENT FIELD DEVICES



**WO 00/77585 A1**



(57) Abstract: Device configurations are stored in a system including at least two intelligent field devices (IFDs) connected by a communications connection. A configuration for a first IFD is stored in the first IFD, and a backup of the configuration for the first IFD is stored in at least one other IFD. Storing a configuration for the first IFD may include having the first IFD request a configuration from at least one other IFD using the communications connection, an IFD having a stored backup of the configuration for the first IFD transmitting the backup to the first IFD using the communications connection, and the first IFD receiving the transmitted backup and storing the received backup in the first IFD as the configuration for the first IFD. Storing a backup of the configuration for the first IFD may include having the first IFD transmit a backup of the configuration for the first IFD to at least one other IFD using the communications connection, and having the at least one other IFD receive and store the backup of the configuration.



patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

**Published:**

— *With international search report.*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

## PEER-TO-PEER HOSTING OF INTELLIGENT FIELD DEVICES

### BACKGROUND

5 Intelligent Field Devices (IFDs) are programmable hardware devices that are commonly used in industrial environments. Examples of IFDs include temperature sensors, pressure sensors, and valve positioners. In a typical industrial setting, there may be many independent IFDs, each of which has a configuration that is customized for the requirements of that IFD. A configuration includes instructions regarding the initial settings of the IFD and the manner in which the IFD will respond to anticipated events. Typically, the  
10 configuration of a particular IFD differs from configurations of other IFDs. A configuration can be updated as often as necessary to provide optimal IFD and system performance.

In one approach to configuring IFDs, a different configurator is used for each IFD. Typically, a configurator is a vendor-supplied, hand-held device that may be connected directly to an IFD.

15 Often, an IFD must recover its configuration due to a power loss, or after replacement due to device failure. A power loss may be planned, as when an IFD is taken out of service for maintenance, or unplanned, as when a power outage occurs. A common approach to recovery from a loss of power is to store the configuration data in non-volatile memory in the IFD. For large IFDs, it often is not practical to provide a sufficient amount of non-volatile  
20 memory within the device itself, due to size, speed, or cost constraints. Therefore, the configuration data for larger IFDs often are stored on a computer and downloaded to the IFD when needed.

25 When an IFD is replaced due to device failure, its configuration must be restored from outside the IFD. The most commonly used method for restoring configurations to an IFD is through a hand-held configurator. In particular, a hand-held configurator stores the configuration for a particular IFD on a removable medium, such as a memory pack. When that IFD is replaced, the corresponding configurator and memory pack are employed to reload the configuration onto the IFD.

30 A common alternative method for IFD configuration recovery is the use of a computer as a central configurator that stores all of the configurations. Typically, a portable computer is used for this purpose. To configure an IFD, the computer is connected to the IFD and the configuration is downloaded from the computer to the IFD. Often, for the sake

of redundancy, a vendor provides both a hand-held configurator and a central configurator system using a portable computer.

## SUMMARY

5 The invention is directed to storing device configurations in a system including at least two interconnected intelligent field devices (IFDs). At least two IFDs and a communications connection between them are provided. A configuration for a first IFD is stored in the first IFD, and a backup of the configuration for the first IFD is stored in at least one other IFD. The configuration for an IFD includes instructions regarding the initial  
10 settings of the IFD and the manner in which the IFD should respond to particular events.

15 Embodiments may include one or more of the following features. For example, storing a configuration for the first IFD may include having the first IFD request a configuration from at least one other IFD using the communications connection, having an IFD with a stored backup of the configuration for the first IFD transmit the backup to the first  
20 IFD using the communications connection, and having the first IFD receive the transmitted backup and store the received backup in the first IFD as the configuration for the first IFD. Additionally, storing a backup of the configuration for the first IFD may include having the first IFD transmit a backup of the configuration for the first IFD to at least one other IFD using the communications connection, and having the at least one other IFD receive and store the backup of the configuration.

25 In another implementation, storing a backup of the configuration for the first IFD includes having the first IFD transmit a backup of the configuration for the first IFD to at least one other IFD using the communications connection, and having the at least one other IFD receive and store the backup of the configuration.

30 In another implementation, storing a configuration for an IFD includes generating the configuration using a configurator program and storing the generated configuration. The configurator program may be stored in an IFD, possibly in the form of a Java applet. The configurator program may be accessed by using a Web browser, which may be stored in a device that is connected to the communications connection, thus enabling the Web browser to access the configurator program through the communications connection.

Alternatively, the Web browser may access the configurator program through a wireless connection between a device on which the Web browser is stored and an IFD. Such

a wireless connection may be accomplished via an infrared connection, using, for example, a personal digital assistant or a portable computer.

5 In another implementation, the configurator program may itself be stored on a Web site. A Web browser may be used to access the configurator program, or an Internet gateway component may be used to access the configurator program by translating the Internet-compatible communications into a protocol being used by the IFDs. Likewise, a backup of the configuration for each IFD may be stored on a Web site, and either a Web browser may be used to access the backup configurations for each IFD, or an Internet gateway component may be used to access the backup configurations for each IFD by translating the Internet-compatible communications into a protocol being used by the IFDs.

10

Storing the backup of the configuration for the first IFD may include storing the backup in at least two other IFDs.

15 Each IFD may include one or more sensors for sensing a process condition or a mechanism for controlling a process condition.

15 The communications connection may include a two-wire connection between the IFDs. The method may further include providing operating power to at least one IFD through the two-wire connection.

20 The peer-to-peer hosting method provides several advantages. The first such advantage is the storage of a configurator within an IFD as a Java applet. This feature obviates the need to employ either a hand-held configurator for each IFD or a central configurator (i.e., a portable computer that contains all of the IFD configurations). This prevents confusion that may arise when associating a hand-held configurator with the IFD for which the hand-held configurator is designed. Because Java is platform-independent, it avoids any incompatibility that might otherwise arise between a hand-held configurator and an IFD. The use of a Java applet as a configurator also removes the need for multiple configurator devices. This reduces the cost of both the IFD vendor and the IFD customer because, at most, only one configurator device is needed. This also eliminates work associated with loading the configurator software onto each portable computer used as a central configurator or each hand-held configurator each time that a new IFD configuration is created.

25

30 Another advantage results from the use of peer IFDs to provide backup configurations for each other, and the use of an automatic configuration reload program. This is particularly

important in the case of device failure and replacement, because the storage of the backup configuration enables the proper configuration to be loaded into the replacement device quickly and automatically. Because there is no need to locate a removable memory pack, problems associated with memory packs, such as swapping or mislabeling, are eliminated.

5 The automation provided by this feature also enables a faster and less expensive configuration recovery, because there is no need to perform the manual operation of reloading the configuration with a hand-held device.

10 The Web browser connection feature provides two advantages. The first advantage is the ability to initialize all of the IFDs from a common source, as opposed to initializing each IFD from a separate hand-held configurator. The second advantage is the ability to archive the configurations in a single, easily accessed repository, such as a Web page maintained by a corporate IFD user. This allows them to be harvested at once and preserved in a safe location.

15 Other features and advantages will be apparent from the following description, including the drawings, and from the claims.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a system for configuring Intelligent Field Devices (IFDs) using configurators that are resident on the IFDs and a portable computer.

20 Fig. 2 is a block diagram of a system for configuring IFDs using resident Java applet configurators and a hand-held personal digital assistant.

Fig. 3 is a block diagram of a system for configuring IFDs using resident Java applet configurators and an Internet/Intranet gateway connection.

25 Fig. 4 is a block diagram of a system for configuring IFDs using a web server from either the Internet or an Intranet as a configurator.

Fig. 5 is a block diagram of a system for configuring IFDs using a network-based approach.

Fig. 6 is a block diagram of a system for configuring IFDs using a network-based approach in which the configurator is resident on the network server.

30 Fig. 7 is a block diagram of a system for configuring IFDs using a network-based approach in which an Internet/Intranet gateway provides a conversion to enable compatibility with non-internet industrial protocols.

Fig. 8 is a flowchart of a peer-to-peer hosting method for configuring IFDs.

#### DETAILED DESCRIPTION

Referring to Figs. 1 and 2, a simple network 100 includes two IFDs, IFD1 105 and IFD2 110. It is noted that the system 100 can easily be adapted to include as many IFDs as desired. The network connections for the network 100 can be either direct electrical connections (i.e., wires) or wireless communications links.

The IFDs in the network use a vendor-selected protocol to format data for transmission to each other, as well as to other electronic devices in the network. Because of the industrial nature of the environments in which IFDs are typically used, some protocols are not designed for Internet access. Examples of such protocols commonly used in typical industrial environments include HART, FoxComm, PROFIBUS, and Foundation Fieldbus. However, in some cases, IFDs use Internet-compatible protocols such as TCP/IP and UCP/IP. In some implementations, one or more IFDs may support multiple protocols.

Typically, each IFD performs a sensing operation, a control operation, or both. IFDs that perform sensing operations, such as temperature sensors, pressure sensors, and flow meters, include one or more sensors for sensing process conditions. In addition to the sensors, these IFDs include transmitter circuitry for transmitting information about the process conditions to other devices.

IFDs that perform control operations, such as valve controllers, include one or more mechanisms for controlling process conditions. These IFDs often receive and use measurement signals provided by sensing IFDs. For example, a valve controller might control the position of a valve in response to a flow rate measurement provided by a flow meter. IFDs may include both sensors and mechanisms for controlling process conditions.

IFDs often are interconnected by two-wire connections. A two-wire connection may be used to provide a communications connection between the IFDs. Many IFDs also receive operating power from an associated two-wire connection.

A configurator program for IFD1 105 can be stored within IFD1 105 as a resident configurator software application 115 (e.g., a Java applet), and a resident configurator software application 120 for IFD2 110 can be stored within IFD2 110. These resident configurator applications can be accessed using a processor, such as, for example, a hand-held device 122 such as a personal digital assistant (e.g., a Palm III), or a portable computer

123, in communication with the IFD through, for example, a direct electrical connection or an infrared link. The configurator program of an IFD can be used to generate a configuration for the IFD. First, the processor downloads the configurator program from the IFD. The processor then runs the configurator program and generates a configuration file in response to inputs to the program from a user. Finally, the processor uploads the configuration file to the IFD, which stores the configuration in the memory of the IFD. Thus, a configuration 125 for IFD1 105 is stored in the memory of IFD1 105, and a configuration 130 for IFD2 110 is stored in the memory of IFD2 110.

5           In some implementations, each IFD can be programmed to store a backup version of its configuration on one or more peer devices. Thus, in the system of Fig. 2, a backup version 140 of the configuration for IFD1 105 is stored on IFD2 110, and a backup version 135 of the configuration for IFD2 110 is stored on IFD1 105. Typically, a backup configuration is generated each time an IFD's configuration is modified.

10           Each IFD also can be programmed to automatically check for the presence of a backup configuration at a peer IFD whenever it has lost power, either due to an outage or due to device failure and replacement. For example, upon power-up, an IFD might be programmed to broadcast a configuration request message identifying the IFD by network address and directed to all peer devices. An IFD having a backup configuration for the broadcasting IFD would respond by sending that backup configuration to the broadcasting IFD. The sending IFD also might include a backup copy of its own configuration for storage 15 on the broadcasting IFD.

15           Referring to Fig. 3, a peer-to-peer hosting system 300 uses a network approach to interconnect three exemplary IFDs. Again, it is noted that the system 300 can easily be adapted to include as many IFDs as desired. IFD1 305, IFD2 310, and IFD3 315 are 20 networked together and include associated Java applet configurators 323, 325, 330. A Java applet configurator can be used to configure each IFD, which then stores its own configuration in memory. Hence, IFD1 305 stores its own configuration 335 in memory, IFD2 310 stores its own configuration 340 in memory, and IFD3 315 stores its own configuration 345 in memory. Additionally, each of the three IFDs can store a backup 25 configuration of another IFD's configuration. For example, IFD1 305 stores the backup configuration 350 for IFD2 310; IFD2 310 stores the backup configuration 355 for IFD3 315; and IFD3 315 stores the backup configuration 360 for IFD1 305. Each IFD can also store 30

software to automatically reload the respective backup configuration when necessary. In another implementation, an IFD may store backup configurations for multiple IFDs, and the backup configuration for an IFD may be stored on multiple IFDs.

5 The system 300 may also include a gateway connection 320 to either the Internet or a stand-alone local area network such as an Intranet. The gateway connection 320 may include browser software 321 for browsing network web sites, such as web sites that may be found on the World Wide Web. The Internet/Intranet gateway 220 can be connected to any IFD on the network. In Fig. 3, the Internet/Intranet gateway 320 is connected to IFD1 305. In some implementations, the Internet/Intranet gateway 320 may provide access to the World Wide 10 Web, thus allowing any web site that contains IFD configuration information to be visited. A web site may even be developed specifically for the purpose of storing and/or supplying IFD configurations. In this manner, a web server can act as a configurator. Referring also to Fig. 4, the use of a web site as a configurator allows this approach to be used in implementations in which the IFDs do not use resident configurator software.

15 The Internet/Intranet gateway 320 can be used to perform the initial generation of an IFD configuration, which may be required when a new IFD is introduced into the system, when an existing IFD requires an update to its configuration, or when a power outage or other event affects all of the IFDs so that they all require configuration reloading. In some implementations, the ability to access the Internet via Web browser software 321 provides 20 system redundancy for configurators as well as backup versions of specific configurations.

Referring to Fig. 5, another implementation of a peer-to-peer hosting system 500 uses a network-based approach. The system 500 includes three exemplary IFDs: IFD1 505, IFD2 510, and IFD3 515. Again, the system 500 can easily be adapted to include as many IFDs as desired. The system 500 also includes a network server 520 with a permanent 25 Internet/Intranet gateway connection 525, including browser software 527. This arrangement provides a robust network design, much like a typical local area network (LAN) or wide area network (WAN). In the system 500, the Internet/Intranet gateway connection 525 allows the configurations to be restored via the gateway 525 for any contingency, so that the 30 configurations can be restored either via the gateway 525 or via the backup configurations 560, 565, 570 stored on corresponding peer devices. Additionally, the backup configurations may be stored on the network server 520, thus providing a third possible source for restoring configurations.

Referring to Fig. 6, in a variation of the implementation illustrated in Fig. 5, the system 500 may still use a network-based approach, but, because it uses an industrial protocol that supports peer-to-peer functionality but is not designed for use with the Internet, such as Foundation Fieldbus or PROFIBUS, there is no gateway connection 525. Despite 5 this, the network-based approach still provides the ability to restore the IFD configurations either from the backup versions on corresponding peer devices via the network server 520, or directly from the network server 520 itself.

This implementation also functions in the absence of resident Java applet 10 configurators by using a configurator 605 that is contained within the network server 520. Once again, system redundancy for both the configurator function and the backup of specific individual configurations is provided, in this instance via the network server 520 and its 15 associated configurator 605.

Referring to Fig. 7, in another variation of the implementations illustrated in Figs. 5 and 6, the system 500 may still use a network-based approach while using an industrial 20 protocol that is not designed for use with the Internet, such as HART, FoxComm, Foundation Fieldbus, or PROFIBUS. Instead of direct access to the Web via browser software 527, the gateway connection 525 contains protocol translation software 705 that translates communications between an Internet-compatible protocol and the local industrial protocol. This variation thus provides the ability to use the Internet as either a configurator or to store 25 backup configurations even when the local protocol does not support Internet communications.

Referring to Figs. 6 and 7, another variation allows the network-based approach to be used even if the local industrial protocol (e.g., HART or FoxComm) does not support peer-to-peer functionality. Thus, in this variation, backup configurations are not stored on peer 25 IFDs. However, configurations can still be provided or restored either by using configurator software 605 that is resident on the network server 520, as shown in Fig. 6, or by using configurator software stored on a web server and accessed via the gateway connection 525, the protocol translation software 705, and the browser software 527, as shown in Fig. 7.

Referring to Fig. 8, an IFD in a system using the peer-to-peer hosting method may 30 operate according to a procedure 800. Initially, the IFD checks whether it is configured (step 805). If the IFD is configured, the IFD proceeds with normal operations (step 810). The IFD

continues with normal operations until a failure, activation of the configurator, or some other event causes the IFD to cease normal operations.

5 If the IFD is not configured, the IFD will request a copy of its configuration from one or more peer devices (step 815). The request may be directed, for example, to a particular peer IFD, the identity of which is pre-loaded in the IFD. The request also may be a broadcast request directed to all peer IFDs.

10 In general, an IFD will receive a configuration from a peer IFD when the IFD has previously lost its configuration due to device failure or replacement, or due to a localized loss of power. When an IFD is connected to the network for the first time, there will not be a backup configuration available for that IFD. However, in some implementations, the IFD 15 may still receive a configuration from a peer IFD. For example, a system may employ a standard configuration for a certain class of IFDs (e.g., pressure sensors), and the IFD may receive a configuration for the class to which it belongs.

15 If the IFD does not immediately receive a copy of its configuration (step 820), the IFD checks to see whether its configurator has been activated (step 825). The configurator may be activated, for example, by a Web browser connected to the IFD or the network including the IFD, by a hand-held device or computer connected to the IFD, or by manipulation of a button or switch mounted on the IFD.

20 If the configurator has been activated, the IFD generates a configuration using the configurator (step 830). After the configuration is generated, the IFD stores the configuration (step 835) and transmits a backup copy of the configuration to one or more other IFDs (step 840). The IFD then confirms that the configuration is complete (step 805) and begins normal operations (step 810).

25 If the configurator has not been activated (step 825), the IFD cycles through a loop that checks for receipt of a configuration (step 820) or activation of the configurator (step 825). The IFD continues to do this until one of these events occurs.

30 If a configuration is received from a peer IFD (step 820), the IFD stores the configuration (step 835). Storage of the configuration may include storage of a backup configuration for the peer IFD transmitted by the peer IFD along with the requested configuration. After storing the configuration, the IFD may optionally transmit a backup copy of its configuration for storage at one or more peer IFDs (step 840). The IFD then

confirms that the configuration is complete (step 805) and begins normal operations (step 810).

5

Upon completion of normal operations, the IFD checks to see if the configurator has been activated (step 845). If so, the IFD generates a revised configuration using the configurator (step 830) and proceeds as discussed above. If not, the IFD verifies that it is still configured (step 805) and proceeds accordingly.

Other embodiments are within the scope of the following claims.

What is claimed is:

1           1. A method of storing device configurations in a system including at least two  
2 interconnected intelligent field devices (IFDs), the method comprising:  
3           providing at least two IFDs;  
4           providing a communications connection between the IFDs;  
5           storing a configuration for a first IFD in the first IFD; and  
6           storing a backup of the configuration for the first IFD in at least one other IFD.

1           2. The method of claim 1, wherein storing a configuration for the first IFD  
2 comprises:  
3           the first IFD requesting a configuration from at least one other IFD using the  
4 communications connection;  
5           an IFD having a stored backup of the configuration for the first IFD transmitting the  
6 backup to the first IFD using the communications connection; and  
7           the first IFD receiving the transmitted backup and storing the received backup in the  
8 first IFD as the configuration for the first IFD.

1           3. The method of claim 2, wherein storing a backup of the configuration for the first  
2 IFD comprises:  
3           the first IFD transmitting a backup of the configuration for the first IFD to at least one  
4 other IFD using the communications connection; and  
5           the at least one other IFD receiving and storing the backup of the configuration.

1           4. The method of claim 1, wherein storing a backup of the configuration for the first  
2 IFD comprises:  
3           the first IFD transmitting a backup of the configuration for the first IFD to at least one  
4 other IFD using the communications connection; and  
5           the at least one other IFD receiving and storing the backup of the configuration.

1        5. The method of claim 1, wherein the configuration includes instructions regarding  
2        the initial settings of the IFD and the manner in which the IFD should respond to particular  
3        events.

1        6. The method of claim 1, wherein storing a configuration for the first IFD comprises  
2        generating the configuration using a configurator program and storing the generated  
3        configuration.

1        7. The method of claim 6, wherein the configurator program is stored in the first IFD.

1        8. The method of claim 7, wherein the configurator program comprises a Java applet.

1        9. The method of claim 7, further comprising accessing the configurator program  
2        using a Web browser.

1        10. The method of claim 9, wherein the Web browser is not stored in the first IFD.

1        11. The method of claim 10, wherein the Web browser is stored in a device  
2        connected to the communications connection and the Web browser accesses the configurator  
3        program through the communications connection.

1        12. The method of claim 10, wherein the Web browser accesses the configurator  
2        program through a wireless connection between a device on which the Web browser is stored  
3        and the first IFD.

1        13. The method of claim 12, wherein the wireless connection comprises an infrared  
2        connection.

1           14. The method of claim 12, wherein the device comprises a personal digital  
2   assistant.

1           15. The method of claim 12, wherein the device comprises a portable computer.

1           16. The method of claim 6, wherein the configurator program is stored on a Web site.

1           17. The method of claim 6, wherein a Web browser is used to access the configurator  
2   program.

1           18. The method of claim 6, wherein an Internet gateway component is used to access  
2   the configurator program by translating Internet-compatible communications into a protocol  
3   being used by the at least two IFDs.

1           19. The method of claim 1, wherein storing the backup of the configuration for the  
2   first IFD comprises storing the backup in at least two other IFDs.

1           20. The method of claim 1, wherein each IFD includes at least a sensor for sensing a  
2   process condition or a mechanism for controlling a process condition.

1           21. The method of claim 1, wherein the communications connection comprises a two-  
2   wire connection between the IFDs.

1           22. The method of claim 21, further comprising providing operating power to at least  
2   the first IFD through the two-wire connection.

1           23. A network of intelligent field devices, the network comprising:  
2        at least two interconnected intelligent field devices (IFDs);  
3        a communications connection between the IFDs;  
4        a configuration for a first IFD stored in the first IFD; and  
5        a backup of the configuration for the first IFD stored in a second IFD.

1           24. The device network of claim 23, wherein the first IFD is configured to request a  
2        configuration from the second IFD using the communications connection, the second IFD is  
3        configured to transmit the backup to the first IFD using the communications connection, and  
4        the first IFD is configured to receive the transmitted backup and to store the received backup  
5        in the first IFD as the configuration for the first IFD.

1           25. The device network of claim 24, wherein the first IFD is configured to transmit a  
2        backup of the configuration for the first IFD to at least the second IFD using the  
3        communications connection, and the second IFD is configured to receive and store the  
4        backup of the configuration.

1           26. The device network of claim 23, wherein the first IFD is configured to transmit a  
2        backup of the configuration for the first IFD to at least the second IFD using the  
3        communications connection, and the second IFD is configured to receive and store the  
4        backup of the configuration.

1           27. The device network of claim 23, wherein the configuration includes instructions  
2        regarding the initial settings of the IFD and the manner in which the IFD should respond to  
3        particular events.

1        28. The device network of claim 23, further comprising a configurator operable to  
2    generate the configuration.

1        29. The device network of claim 28, wherein the configurator comprises a program  
2    stored in the first IFD.

1        30. The device network of claim 29, wherein the configurator program comprises a  
2    Java applet.

1        31. The device network of claim 29, wherein the configurator program is configured  
2    to be accessed using a Web browser.

1        32. The device network of claim 31, wherein the Web browser is stored remotely  
2    from the first IFD, the network comprising a connection to the Web browser.

1        33. The device network of claim 32, wherein the Web browser is stored in a device  
2    connected to the communications connection and is configured to access the configurator  
3    program through the communications connection.

1        34. The device network of claim 32, wherein the Web browser is configured to  
2    access the configurator program through a wireless connection between a device on which  
3    the Web browser is stored and the first IFD.

1        35. The device network of claim 34, wherein the wireless connection comprises an  
2    infrared connection.

1        36. The device network of claim 34, wherein the device on which the Web browser is  
2    stored comprises a personal digital assistant.

1        37. The device network of claim 34, wherein the device on which the Web browser is  
2        stored comprises a portable computer.

1        38. The device network of claim 28, wherein the configurator program is stored on a  
2        Web site.

1        39. The device network of claim 28, wherein the configurator program is configured  
2        to be accessed using a Web browser.

1        40. The device network of claim 28, further comprising an Internet gateway  
2        component for use in accessing the configurator program by translating Internet-compatible  
3        communications into a protocol being used by the first IFD.

1        41. The device network of claim 23, further comprising a third IFD and a second  
2        backup of the configuration for the first IFD, the second backup being stored in the third IFD.

1        42. The device network of claim 23, wherein each IFD includes at least a sensor for  
2        sensing a process condition or a mechanism for controlling a process condition.

1        43. The device network of claim 23, wherein the communications connection  
2        comprises a two-wire connection between the IFDs.

1        44. The device network of claim 43, wherein the two-wire connection is connected to  
2        provide operating power to at least the first IFD.

1           45. Software, residing on a processor-readable medium, for storing device  
2 configurations in a system including at least two intelligent field devices (IFDs)  
3 interconnected by a communications connection between the IFDs, the software comprising  
4 instructions for causing the system to:  
5           store a configuration for a first IFD in the first IFD; and  
6           store a backup of the configuration for the first IFD in at least one other IFD.

1           46. A method of installing a device configuration on an intelligent field device (IFD),  
2 the method comprising: storing a configurator program on the IFD; using an external  
3 processor to access the configurator program; running the configurator program on the  
4 external processor to generate the device configuration; transmitting the device configuration  
5 to the IFD; and storing the device configuration in memory in the IFD.

1           47. The method of claim 46, wherein the configurator program comprises a Java  
2 applet.

1           48. The method of claim 46, wherein the external processor comprises a personal  
2 computer.

1           49. The method of claim 46, wherein the external processor comprises a hand-held  
2 device.

1           50. A method of installing a device configuration on an IFD, the method comprising:  
2 storing a configurator program on a distributed network site; accessing the configurator  
3 program using browser software; running the configurator program to generate the device  
4 configuration; and storing the device configuration in memory in the IFD.

1            51. The method of claim 50, wherein the distributed network site comprises a World  
2    Wide Web site.

1            52. The method of claim 51, further comprising translating communications between  
2    a protocol used by the distributed network site and a protocol used by the IFD.

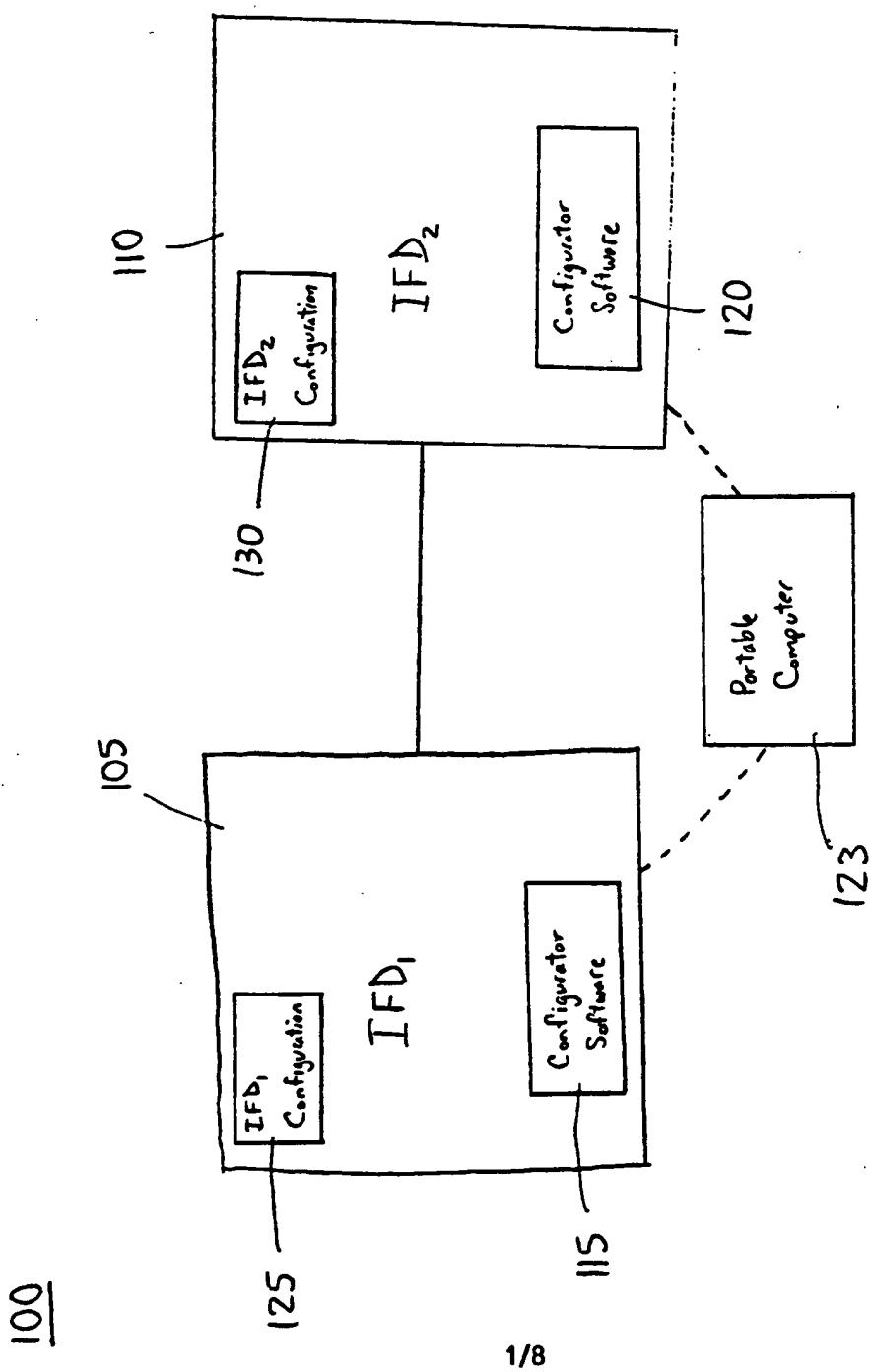


Figure 1

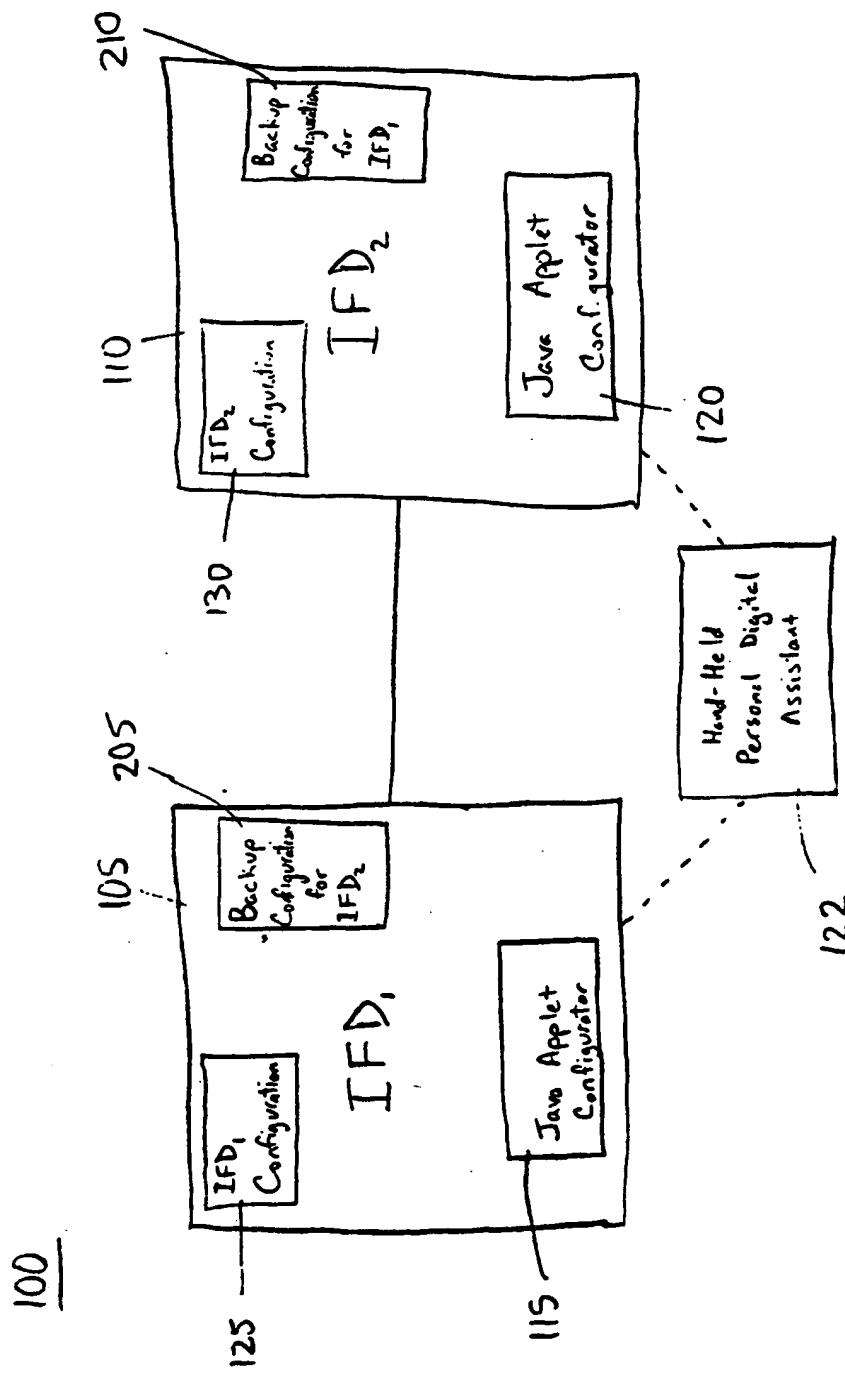


Figure 2

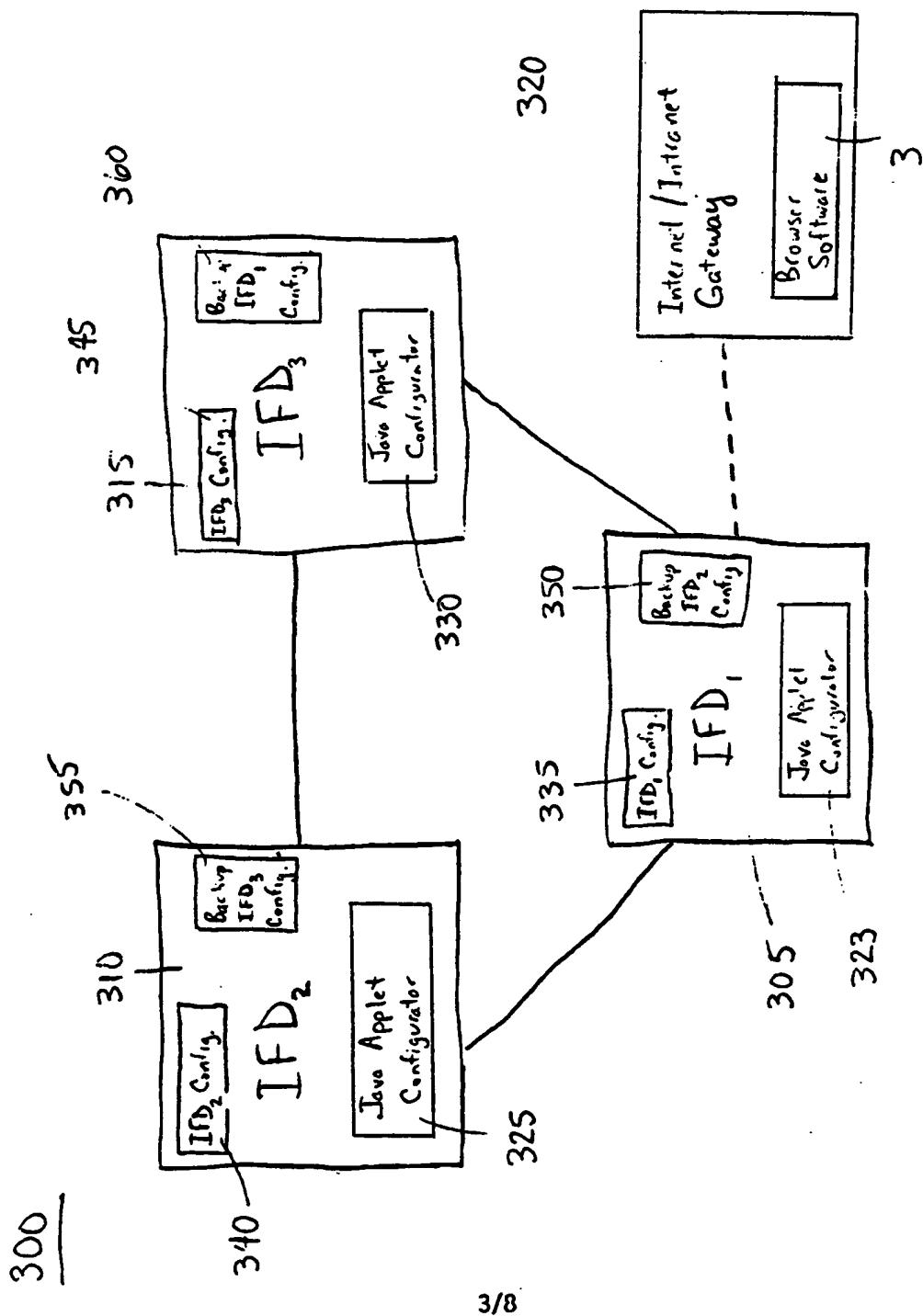


Figure 3

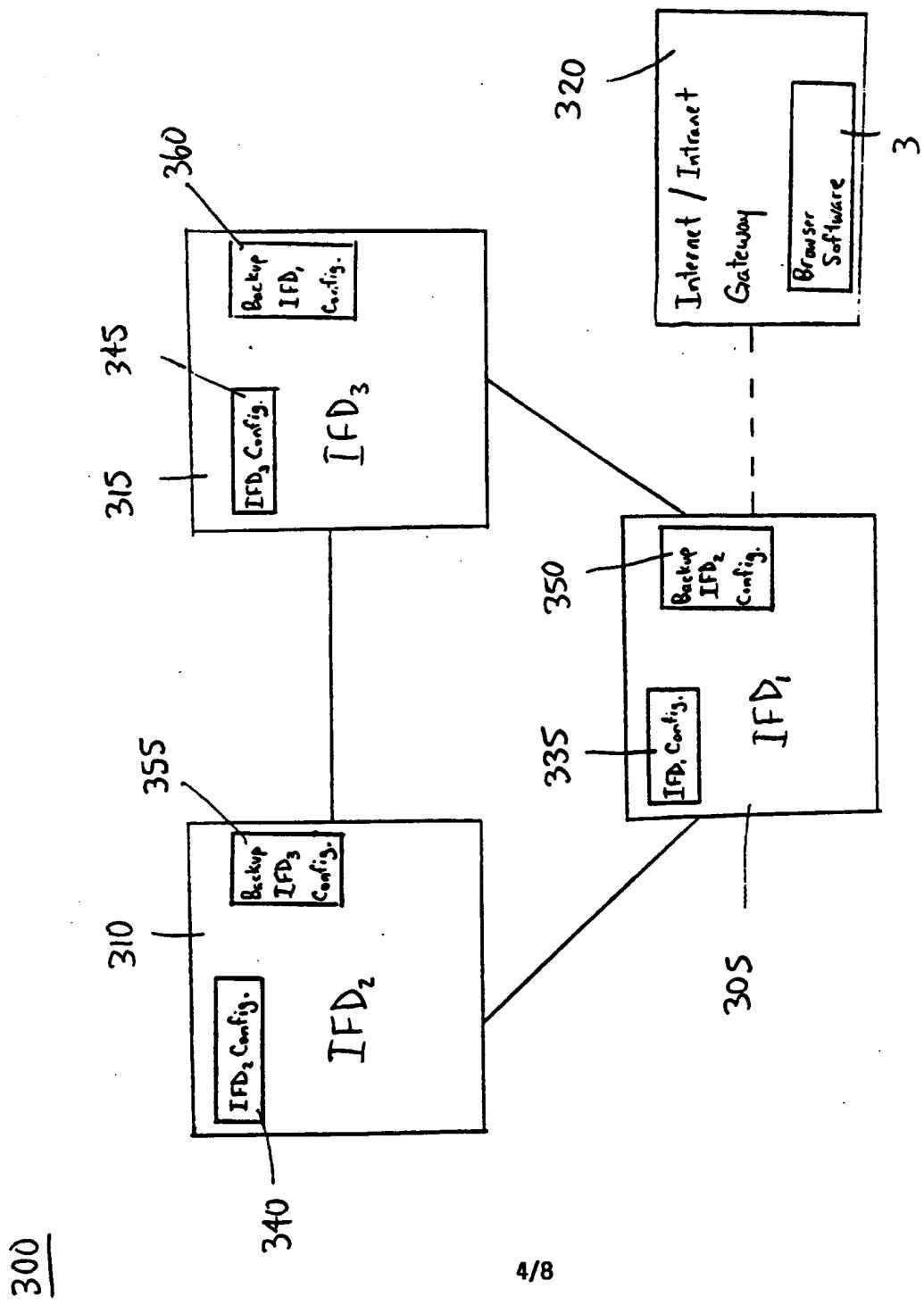


Figure 4

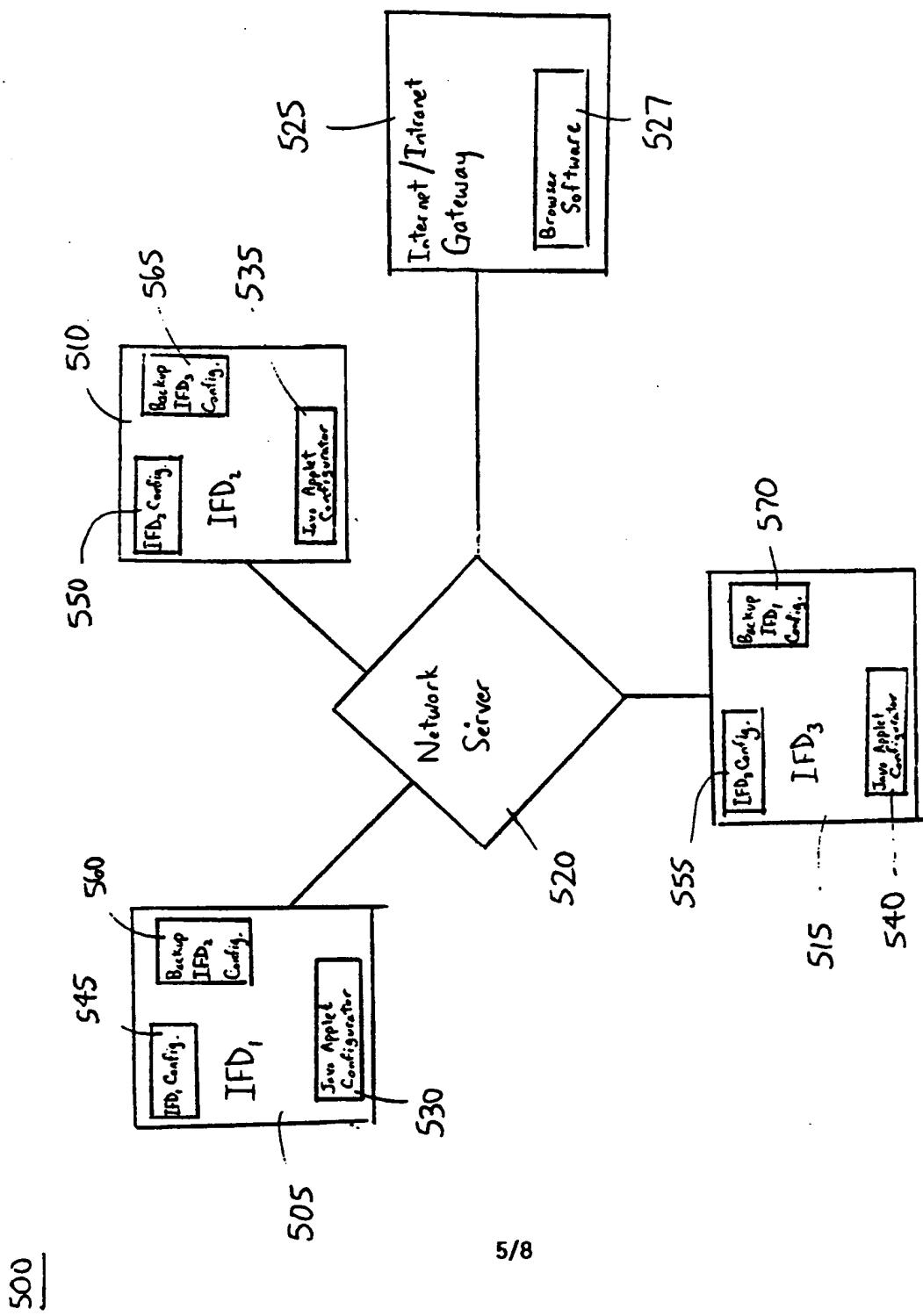


Figure 5

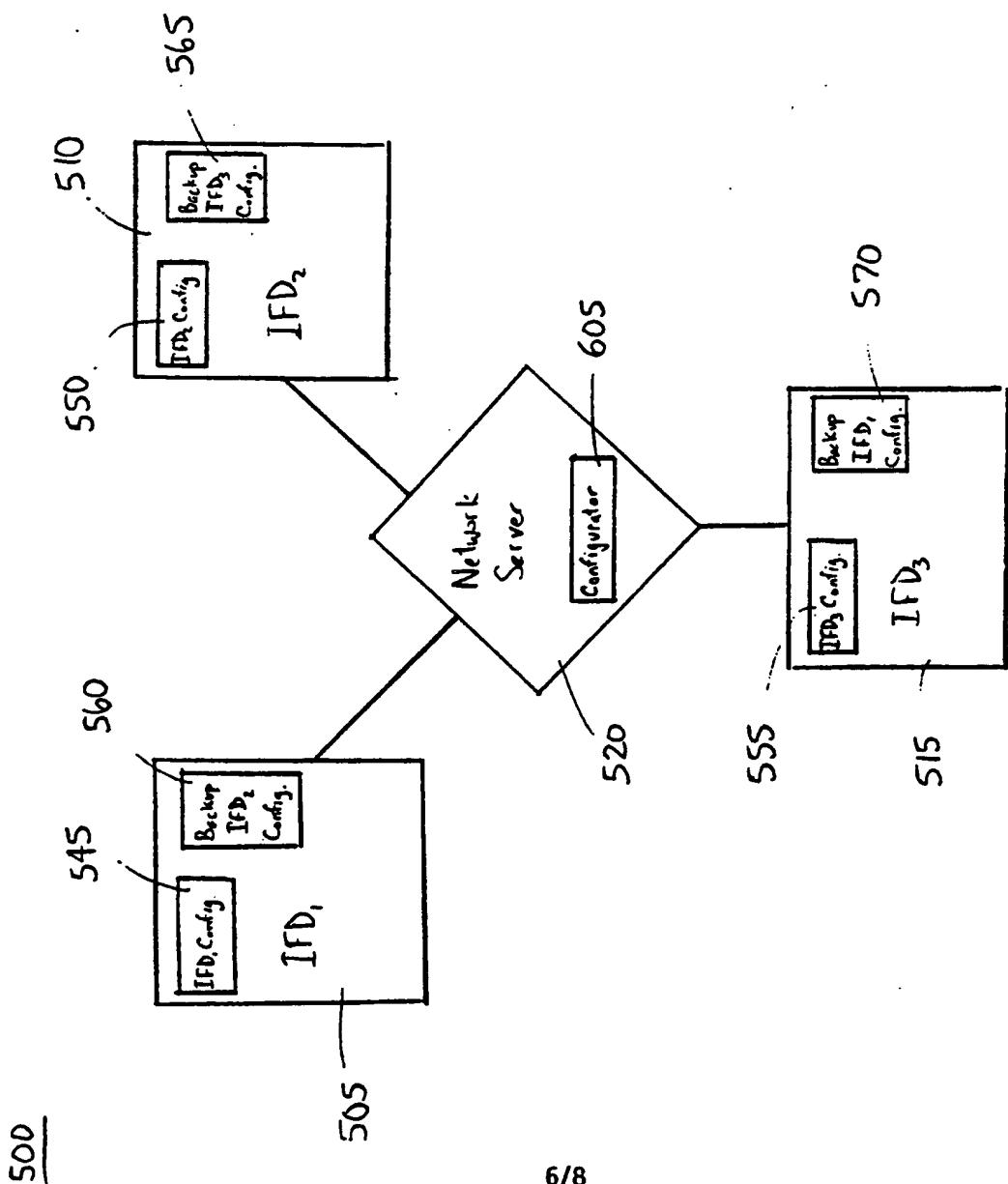


Figure 6

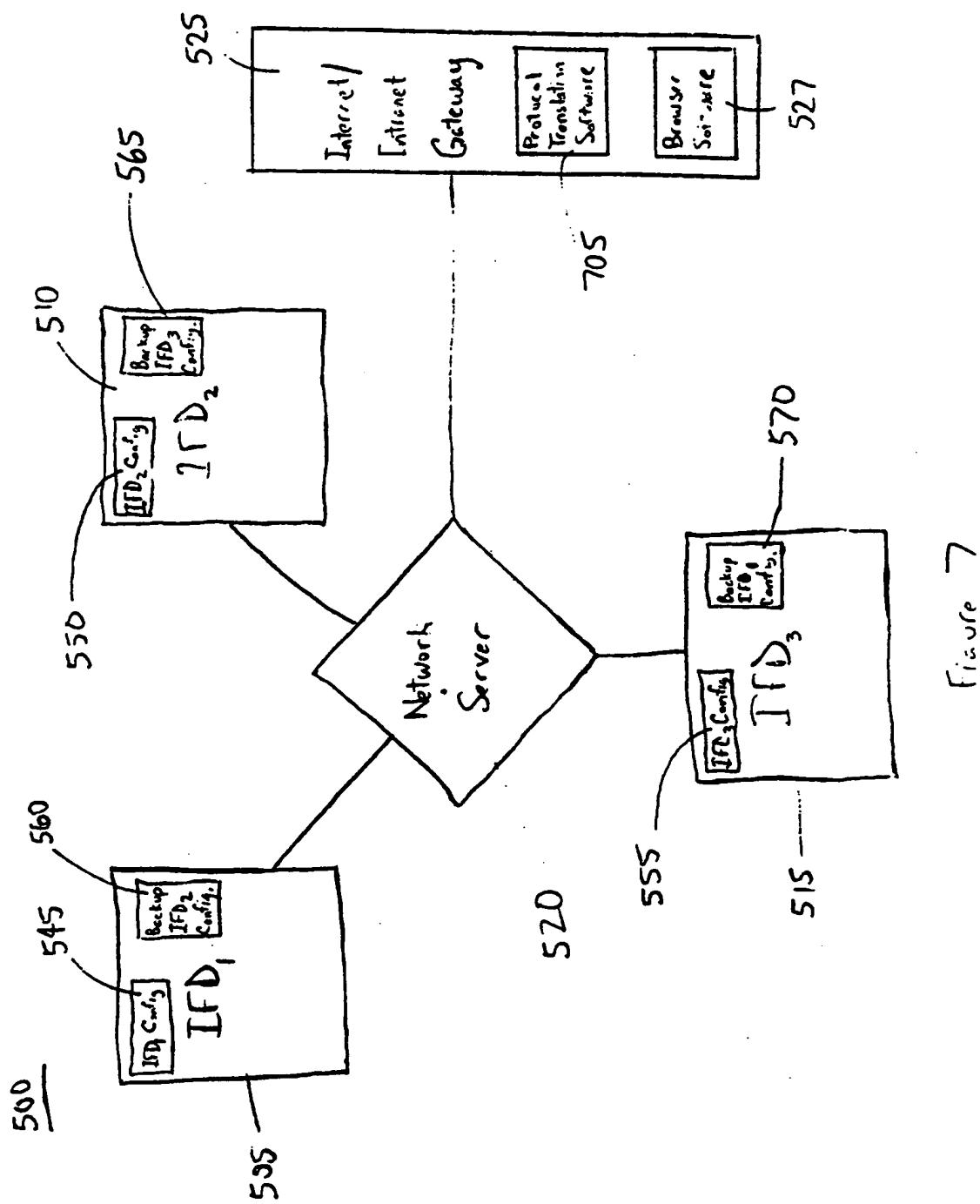


Figure 7

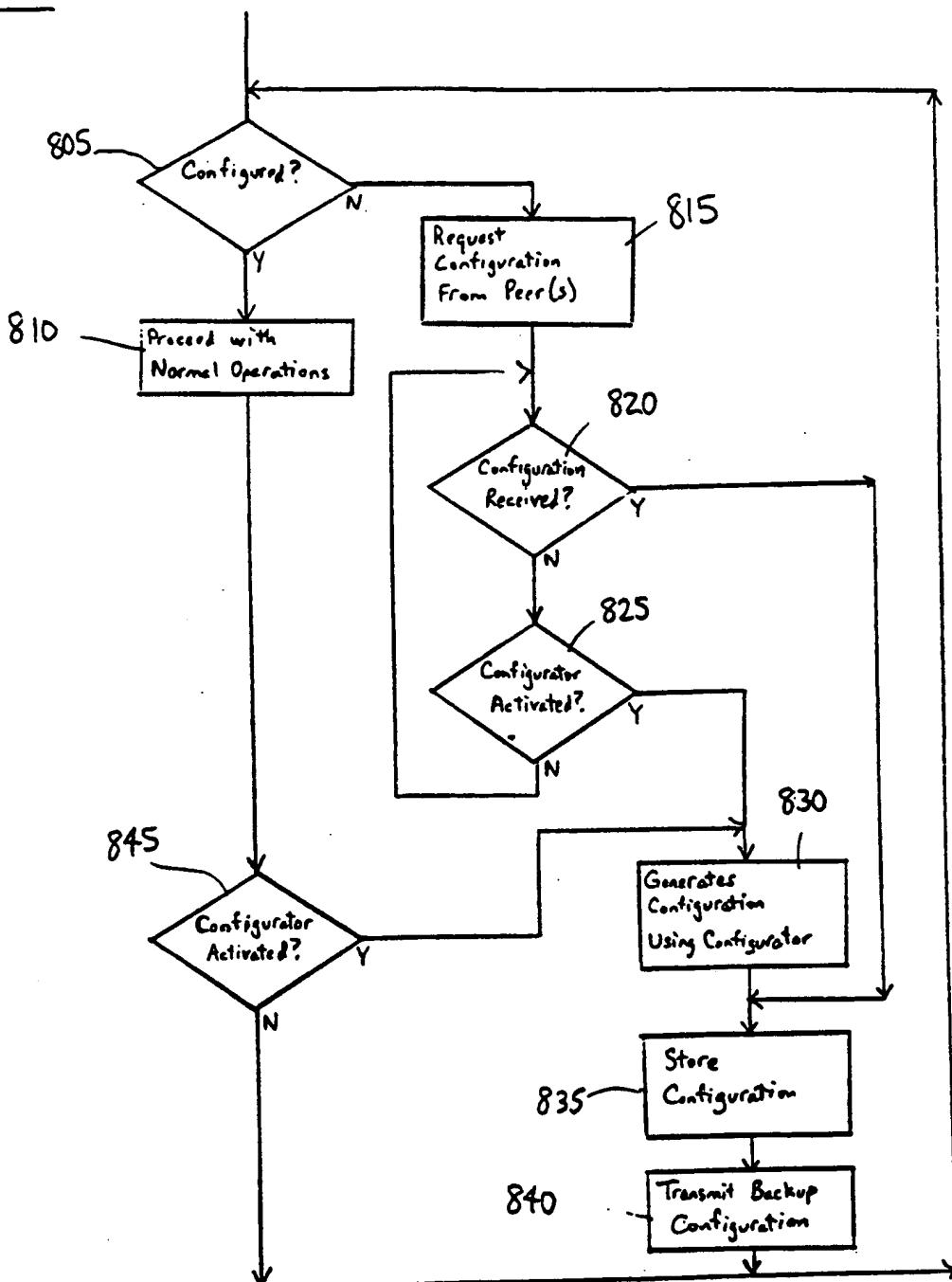
800

Figure 8

# INTERNATIONAL SEARCH REPORT

International Application No  
PCT/US 00/15894

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 G05B19/042 G05B19/05

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 G05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

PAJ, EPO-Internal, WPI Data

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	PATENT ABSTRACTS OF JAPAN vol. 1997, no. 09, 30 September 1997 (1997-09-30) & JP 09 123422 A (MITSUBISHI HEAVY IND LTD), 13 May 1997 (1997-05-13) abstract	1-7, 19, 20, 23-29, 41, 42, 45, 46 8-18, 21, 22, 30-40, 47-52
Y	PRESTON D J: "INTERNET PROTOCOLS MIGRATE TO SILICON FOR NETWORKING DEVICES", ELECTRONIC DESIGN, US, PENTON PUBLISHING, CLEVELAND, OH, VOL. 45, NR. 8, PAGE(S) 87-90, 92-94 XP000730016 ISSN: 0013-4872 figures 1-3	8-18, 21, 22, 30-40, 47-52
	---	-/-

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

\* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

\*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

\*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

\*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

\*&\* document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

23 October 2000

30/10/2000

Name and mailing address of the ISA  
European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl.  
Fax: (+31-70) 340-3016

Authorized officer

Tran-Tien, T

# INTERNATIONAL SEARCH REPORT

Internat'l Application No  
PCT/US 00/15894

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99 20075 A (SHEEHY MORGAN ;KEARNEY ADRIAN (IE); VISERGE LIMITED (IE); DONNELL) 22 April 1999 (1999-04-22) page 8, line 1 -page 14, line 33; figures 1,5 -----	1-7, 23-29
A	US 5 270 917 A (KIMURA YOSHIYUKI) 14 December 1993 (1993-12-14) abstract -----	1-52
A	FUHR P L ET AL: "REMOTE INTERROGATION AND CONTROL OF SENSORS VIA THE INTERNET", SENSORS,US,HELMERS PUBLISHING, VOL. 12, NR. 12, PAGE(S) 25-29,31 XP002050471 ISSN: 0746-9462 the whole document -----	1-52
A	WO 98 53581 A (COACTIVE NETWORKS INC) 26 November 1998 (1998-11-26) abstract -----	1-52
A	WO 98 50834 A (CONTROL TECHNOLOGY CORP) 12 November 1998 (1998-11-12) abstract -----	1-52
A	WO 98 26337 A (WESTINGHOUSE ELECTRIC CORP) 18 June 1998 (1998-06-18) abstract -----	1-52

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

Intern'l Application No  
PCT/US 00/15894

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
JP 09123422	A	13-05-1997	NONE		
WO 9920075	A	22-04-1999	AU	9557198 A	03-05-1999
			EP	1023816 A	02-08-2000
			IE	80817 B	10-03-1999
US 5270917	A	14-12-1993	JP	4101201 A	02-04-1992
			DE	69120168 D	18-07-1996
			DE	69120168 T	20-02-1997
			EP	0472169 A	26-02-1992
WO 9853581	A	26-11-1998	EP	1013047 A	28-06-2000
WO 9850834	A	12-11-1998	US	5982362 A	09-11-1999
			AU	7370098 A	27-11-1998
WO 9826337	A	18-06-1998	US	6070250 A	30-05-2000
			CN	1246183 A	01-03-2000